IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS

SANDRA GLEASON, individually and on behalf of all others similarly situated, Plaintiff, v. METHODIST MCKINNEY HOSPITAL, LLC, Defendant.	CASE NO: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Sandra Gleason ("Gleason"), individually and on behalf of all others similarly situated, bring this action against Defendant Methodist McKinney Hospital, LLC ("MMH") "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused Plaintiff and the approximately 110,224 other similarly situated persons in the massive and preventable cyberattack, in which cybercriminals infiltrated Defendant's inadequately protected computer network where highly sensitive personally identifiable information and protected health information were being kept without sufficient data security protection ("Data Breach" or "Breach").[1]

[1] *See* https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-520.pdf (posting of data breach); *see also* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (showing 110,224 individuals affected by the data breach).

2. Defendant MMH is a for-profit hospital that provides inpatient and outpatient medical services. MMH is part of the Methodist Health System, which operates a network of hospitals and medical centers in north Texas.

3. On information and belief, in the ordinary course of business, MMH collects from its patients personally identifiable information ("PII") and protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA").

4. According to MMH, the information compromised in the Data Breach includes names, addresses, Social Security numbers, dates of birth, medical history information, medical diagnosis and treatment information, health insurance, and/or medical record number (the "Personal and Medical Information").

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address MMH's inadequate safeguarding of Class Members' Personal and Medical Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Personal and Medical Information in a reckless and negligent manner. In particular, the Personal and Medical Information was maintained on MMH's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Personal and Medical Information was a known risk to the Defendant and thus the Defendant was on notice that failing to take steps necessary to secure the Personal and Medical Information from those risks left that information in a dangerous condition.

7. In addition, MMH and its employees failed to properly monitor and/or negligently monitored the computer network and IT systems that housed the Personal and Medical Information.

8. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Personal and Medical Information that Defendant collected and maintained is now in the hands of data thieves.

9. Armed with the Personal and Medical Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. As a result of the Data Breach, Plaintiff and Class Members are exposed to a heightened and imminent risk of fraud and identity theft.

11. Indeed, Russian hackers known as the Karakurt gang have already boasted on the dark web that they acquired 367 gigabytes of sensitive data from Defendant.[2]

12. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

[2] https://www.cbsnews.com/dfw/news/mckinney-hospital-surgical-centers-targeted-by-group-of-russian-hackers/ (last visited September 12, 2022).

13. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. By this Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Personal and Medical Information was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to MMH's data security systems, future annual audits, and adequate medical identification and credit monitoring services funded by Defendant.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful and negligent conduct.

PARTIES

17. Plaintiff Sandra Gleason is a citizen and resident of Ponder, Texas.

18. Defendant MMH is a for-profit hospital located in McKinney, Texas.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant.[3] Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has personal jurisdiction over Defendant because it operates and are headquartered in this District and conduct substantial business in this District.

[3] *See, e.g.*, https://dojmt.gov/consumer/databreach/ (showing 25 Montanans affected by the Data Breach).

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is based in this District, maintains Class Members' Personal and Medical Information in the District, and has caused harm to Class Members from this District.

FACTUAL ALLEGATIONS

A. The Data Breach

22. On July 5, 2022, MMH learned that it was the victim of a cyberattack. Following a forensic investigation, MMH discovered that an unknown cybercriminals had accessed and obtained the Personal and Medical Information of approximately 110,244 individuals. [4]

23. According to the notice of Data Breach letter that MMH sent to state Attorneys General and Plaintiff and Members of the Class on or about August 26, 2022, the information obtained by the cyber attacker included at least: name, address, Social Security number, date of birth, medical history information, medical diagnosis information, medical treatment information, health insurance information, and/or medical record number.[5]

24. Upon information and belief, the Data Breach targeted MMH due to its status as a healthcare provider that collects, creates, and maintains Personal and Medical Information. Moreover, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the Personal and Medical Information of Plaintiff and the Class Members. Because of the Data Breach, data thieves were able to gain access to MMH's IT systems and to access and acquire the unencrypted Personal and Medical Information of Plaintiff and Class Members.

[4] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
[5] https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-520.pdf.

25. In the notices that MMH provided to impacted persons and the states Attorneys General, MMH openly admits that the Personal and Medical Information of Plaintiff and Class Members that was accessed without authorization by hackers and even "copied", according to the notice letter the Data Breach.[6] This means that not only did the cybercriminals view and access the Personal Information without authorization, but they also removed Plaintiff's and Class Members' Personal Information from MMH's network.

26. Due to MMH's inadequate and insufficient data security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever. Plaintiff believes her Personal and Medical Information was both stolen in the Data Breach (a fact admitted by MMH in its notice of Data Breach) and is still in the hands of the hackers. Plaintiff further believes that their Personal and Medical Information was subsequently sold or published on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals who perpetrate cyberattacks of the type that occurred here. In fact, here, Russian hackers are have already posted 360 gigabytes of Personal and Medical Information on the dark web.[7]

27. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its customers' promises and representations made to Plaintiff and Class Members to keep their Personal and Medical Information confidential and to protect it from unauthorized access and disclosure.

28. Plaintiff and Class Members relied on the sophisticated Defendant to keep their Personal and Medical Information confidential and securely maintained, to use this information

[6] https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-520.pdf,
[7] https://healthitsecurity.com/news/karakurt-ransomware-group-targets-methodist-mckinney-hospital-in-cyberattack.

for business and/or medical purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their sensitive Personal and Medical Information.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff' and Class Members' Personal and Medical Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for and had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Personal and Medical Information from involuntary disclosure to third parties.

30. Plaintiff and Class Members entrusted their Personal and Medical Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Due to MMH's inadequate and insufficient data security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever.

B. Plaintiff's Experience

32. Plaintiff Sandra Gleason provided MMH her Personal and Medical Information in order to receive medical services.

33. Plaintiff's Personal and Medical Information was within the possession and control of Defendant at the time of the Data Breach.

34. Plaintiff Gleason received a letter from MMH dated August 26, 2022, informing him that her Personal and Medical Information was involved in the Data Breach. *See* Exhibit 1, attached hereto.

35. As a result of the Data Breach, MMH directed Plaintiff Gleason to take certain steps to protect her Personal and Medical Information and otherwise mitigate her damages.[8]

36. As a result of the Data Breach, Plaintiff Gleason has been forced to spend time dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the breach notification letter, reviewing and self-monitoring her financial accounts statements and other personal information, exploring her options for best protecting herself, securing credit monitoring and identity theft protection services, and taking other continued actions in an attempt to lessen the harms to her as a result of the Data Breach.

37. Even with the best response, the harm caused to Plaintiff and the Class cannot be undone.

38. Russian hackers, known as the Karakurt gang, have already boasted that they acquired 367 gigabytes of Personal and Medical Information from Defendant and have posted on the dark web.[9] Thus, Plaintiff and Class Members' information is already being misused by cybercriminals.

39. Plaintiff is very careful about sharing her own Personal and Medical Information and has never knowingly transmitted unencrypted Personal and Medical Information over the internet or any other unsecured source.

40. Plaintiff suffered actual injury and damages due to Defendant's mismanagement of her Personal and Medical Information before and throughout the Data Breach.

[8] *See* https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-520.pdf; *see also* Exhibit 1 (attached hereto).
[9] https://healthitsecurity.com/news/karakurt-ransomware-group-targets-methodist-mckinney-hospital-in-cyberattack; https://www.cbsnews.com/dfw/news/mckinney-hospital-surgical-centers-targeted-by-group-of-russian-hackers/ (last visited September 12, 2022).

41. Plaintiff suffered actual injury in the form of damages and diminution in the value of her Personal and Medical Information—a form of intangible property that he entrusted to Defendant for the purpose of providing healthcare related services, which was compromised in and as a result of the Data Breach.

42. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with his Social Security number, address, and date of birth.

43. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Personal and Medical Information, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

44. Plaintiff has a continuing interest in ensuring that her Personal and Medical Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

C. The Data Breach was foreseeable

45. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

46. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[10] The 330

[10] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

47. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

48. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

49. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[12]

50. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

[11] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware

[12] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

D. Defendant Failed to Comply with FTC Guidelines

51. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

52. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[13] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

53. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and

[13] [13] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Defendant failed to properly implement basic data security practices.

56. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

57. Defendant was always fully aware of its obligation to protect the PII and PHI of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with Industry Standards

58. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

59. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like MMH, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

60. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such

as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

61. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

62. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

F. Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

63. HIPAA requires covered entities and business associates of covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

64. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

65. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules

include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

66. A Data Breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

67. A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

68. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. *See* 45 C.F.R.164.308(a)(6).[14]

69. Defendant MMH's Data Breach resulted from a combination of insufficiencies that demonstrate MMH failed to comply with safeguards mandated by HIPAA regulations.

[14] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

G. Cybercriminals Have Used and Will Continue to Use Plaintiff and Class Members' PII and PHI for Fraud and Identity Theft

70. PII and PHI are of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

71. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[15] For example, with the Personal and Medical Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[16] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

72. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[17]

---

[15] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[16] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[17] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

73. PII and PHI are such valuable commodities to identity thieves that once this information has been compromised, criminals will use it for years.[18]

74. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against medical service providers like Defendant is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[19] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[20]

75. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[21]

76. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

77. [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[19] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[20] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[21] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

78. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[23]

79. The ramifications of Defendant's failure to keep its Class Members' PII secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

80. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

81. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [24] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[25]

---

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[23] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[24] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[25] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

82. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[26]

83. Defendant's offer of limited identity monitoring to Plaintiff and the Class is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Once the offered coverage has expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendant's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[27] Nor can an identity monitoring service remove personal information from the dark web.[28] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[29]

84. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the

[26] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[27] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

[28] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[29] *Id.*

Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

85. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

86. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

87. Trespass, damage to, and theft of their personal property including PII;

88. Improper disclosure of their PII;

89. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;

90. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;

91. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

92. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

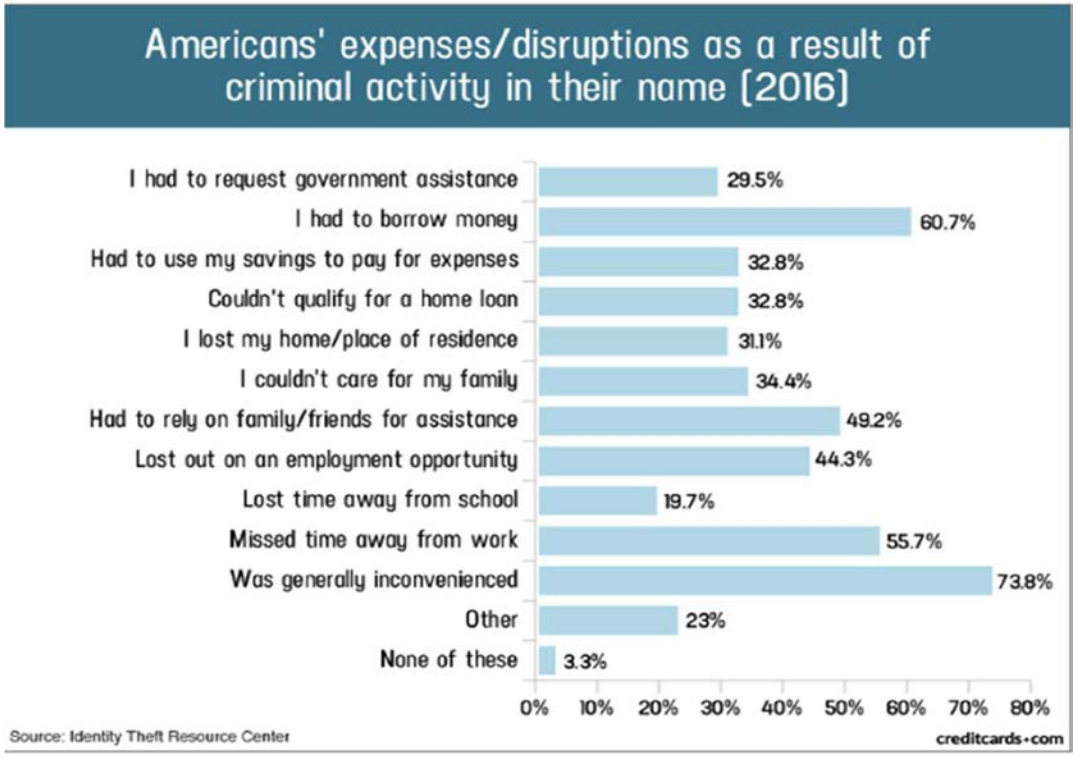
93. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;

94. The loss of use of and access to their credit, accounts, and/or funds;

95. Damage to their credit due to fraudulent use of their PII; and

96. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

97. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[30]:



[30] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

98. Moreover, theft of Personal and Medical Information is also gravely serious. PII and PHI is an extremely valuable property right.[31]

99. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Personal and Medical Information has considerable market value.

100. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[32]

101. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

102. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Personal and Medical Information and/or financial information is stolen and when it is used.

[31] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[32] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft identity-theft (last visited Sept. 12, 2022).

103. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

104. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

105. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

106. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

107. Sensitive Personal and Medical Information can sell for as much as $363 per record according to the Infosec Institute.[34] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

[33] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[34] See Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

108. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[35] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

109. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

110. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security. number."[36]

111. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[37]

---

[35] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

[36] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about- identity-theft (last visited Sept. 12, 2022).

[37] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 12, 2022).

112. Medical information is especially valuable to identity thieves.

113. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

114. For this reason, Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

H. Defendant's negligent acts and breaches

115. MMH breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect the Personal and Medical Information of Plaintiff and the Class;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to train employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to and maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

p. Failing to adhere to industry standards for cybersecurity.

116. As the result of antivirus and malware protection software in need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks like the one here, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Personal and Medical Information by allowing providing unsecured and unencrypted Personal and Medical Information to MMH which in turn allowed cyberthieves to access its IT systems.

117. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

I. Plaintiff's and Class Members' Damages

118. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. MMH has only offered 12 months of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

119. The 12 months of credit monitoring offered to persons whose Personal and Medical Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, MMH places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

120. Plaintiff and Class Members have been damaged by the compromise of their Personal and Medical Information in the Data Breach.

121. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

122. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

123. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Personal and Medical

Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

124. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

125. Plaintiff and Class Members suffered actual injury from having their Personal and Medical Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Personal and Medical Information, a form of property that MMH obtained from Plaintiff; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

126. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

127. Plaintiff and Class Members have been damaged by the compromise of their Personal and Medical Information in the Cyber-Attack. Moreover, Defendant's delay in noticing affected persons of the theft of their PII prevented early mitigation efforts and compounded the harm.

128. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- Purchasing credit monitoring and identity theft prevention;

- Placing "freezes" and "alerts" with reporting agencies;
- Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- Contacting financial institutions and closing or modifying financial accounts; and

129. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

130. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal and Medical Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Personal and Medical Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

131. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

132. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

133. Plaintiff proposes the following Class definition, subject to amendment based on information obtained through discovery:

> All persons whose Personal and Medical Information was maintained on MMH's system that was compromised in the Data Breach and who were sent a notice of the Data Breach (the "Class").

134. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

135. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

136. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

137. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consist of more than 110,000 individuals whose data was compromised in the Data Breach.

138. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personal and Medical Information;

b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c) Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d) Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e) Whether Defendant owed a duty to Class Members to safeguard their Personal and Medical Information;

f) Whether Defendant breached their duty to Class Members to safeguard their Personal and Medical Information;

g) Whether computer hackers obtained Class Members' Personal and Medical Information in the Data Breach;

h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant's conduct was negligent;

k) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

139. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

140. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class and have no interests antagonistic to those of other Class Members. Plaintiff's Counsel are competent and experienced in litigating data breach class actions.

141. Predominance. Defendant engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data were stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

142. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

143. Defendant acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and all Class Members)

144. Plaintiff re-alleges and incorporates by reference each preceding paragraph as if fully set forth herein.

145. Defendant required the submission of Plaintiff's and Class Members Personal and Medical Information as a condition or providing healthcare related services for the benefit of Plaintiff and Class Members. HIPAA covered entities and business associates provided this Personal and Medical Information to Defendant MMH.

146. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Personal and Medical Information for its own pecuniary benefit and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

147. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Personal and Medical Information.

148. Defendant had full knowledge of the sensitivity of the Personal and Medical Information and the types of harm that Plaintiff and Class Members could and would suffer if the data were wrongfully disclosed.

149. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Personal and Medical Information held within it—to prevent disclosure of the information, and to safeguard the

information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt and adequate notice to those affected in the case of a data breach.

150. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

151. Defendant also had a duty to use reasonable security measures under HIPAA which required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

152. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

153. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, including sharing and/or storing the Personal and Medical Information of Plaintiff and Class Members on its computer systems.

154. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal and Medical Information of Plaintiff and Class

Members, the critical importance of providing adequate security of that data, and the necessity for encrypting all data stored on Defendant's systems.

155. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the Personal and Medical Information of Plaintiff and Class Members, including basic encryption techniques freely available to Defendant.

156. Plaintiff and Class Members had no ability to protect their Personal and Medical Information that was in, and possibly remains in, Defendant's possession.

157. Defendant was in a position and able to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

158. Defendant had and continues to have a duty to adequately disclose that the Personal and Medical Information of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal and Medical Information by third parties.

159. Defendant had a duty to comply with the industry standards set out above.

160. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Personal and Medical Information within Defendant's possession.

161. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Personal and Medical Information.

162. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Personal and Medical Information within Defendant's possession might have been compromised and precisely the type of information compromised.

163. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Personal and Medical Information to be compromised.

164. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding the type of Personal and Medical Information that has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

165. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, fraud, loss of time and money to monitor their finances for fraud, and loss of control over their Personal and Medical Information.

166. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Personal and Medical Information, which is still in the possession of third parties, will be used for fraudulent purposes.

167. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal and Medical Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Personal and Medical Information of Plaintiff and Class Members was stolen and accessed as the proximate

result of Defendant's failure to exercise reasonable care in safeguarding such Personal and Medical Information, by adopting, implementing, and maintaining appropriate security measures.

168. Plaintiff seeks an award of actual damages on behalf of themselves and the Class.

169. In failing to secure Plaintiff's and Class Members' Personal and Medical Information and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

170. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information.

COUNT II

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and all Class Members)

171. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

172. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the PHI and PII of Plaintiff and the Class.

173. Defendant is a covered entity under HIPAA, 45 C.F.R. §160.102, and as such is required to comply with the HIPAA's Privacy Rule and Security Rule. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the

privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

174. HIPAA further requires Defendant to disclose the unauthorized access and theft of the protected health information of Plaintiff and the Class "without unreasonable delay" so that Plaintiff and Class members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404, 164.406, and 164.410.

175. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI and PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

176. Defendant gathered and stored the PHI and PII of Plaintiff and the Class as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

177. Defendant violated the FTC Act by failing to use reasonable measures to protect the PHI and PII of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

178. Defendant breached its duties to Plaintiff and the Class under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' PHI and PII, and by failing to provide prompt notice without reasonable delay.

179. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

180. Plaintiff and the Class are within the class of persons that HIPAA and the FTC Act were intended to protect.

181. The harm that occurred as a result of the Data Breach is the type of harm HIPAA and the FTC Act were intended to guard against.

182. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PHI and PII.

183. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

184. Defendant's violation of the FTC Act and HIPAA constitutes negligence *per se*.

185. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

186. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

187. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

COUNT III

INVASION OF PRIVACY
(On Behalf of Plaintiff and all Class Members)

188. Plaintiff re-alleges and incorporates by reference each preceding paragraph as if fully set forth herein.

189. Plaintiff and Class Members had a legitimate expectation of privacy to their PHI and PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

190. Defendant owed a duty to Plaintiff and Class Members to keep their Personal and Medical Information confidential.

191. Defendant intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted Personal and Medical Information of Plaintiff and Class Members.

192. Defendant allowed unauthorized and unknown third parties access to and examination of the Personal and Medical Information of Plaintiff and Class Members, by way of Defendant's failure to protect the Personal and Medical Information.

193. The unauthorized release to, custody of, and examination by unauthorized third parties of the Personal and Medical Information of Plaintiff and Class Members is highly offensive to a reasonable person.

194. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Personal and Medical Information to Defendant as a necessary condition of receiving healthcare or health insurance, but privately with an intention that the Personal and Medical Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

195. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

196. Defendant acted with intention and a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

197. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

198. As a proximate result of the above acts and omissions of Defendant, the Personal and Medical Information of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

199. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Personal and Medical Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and all Class Members)

200. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

201. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their Personal and Medical Information in order for MMH to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' Personal and Medical Information and to timely and adequately notify them in the event of a data breach.

202. Plaintiff and Class Members would not have provided their Personal and Medical Information to Defendant had they known that Defendant would not safeguard their Personal and Medical Information, as promised, or provide sufficiently detailed notice of a data breach.

203. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

204. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' Personal and Medical Information and by failing to provide them with timely and accurate notice of the Data Breach.

205. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

COUNT V

UNJUST ENRICHMENT
(On Behalf of Plaintiff and all Class Members)

206. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

207. Plaintiff and Class Members conferred a monetary benefit to Defendant when they provided their Personal and Medical Information and payment to their healthcare or insurance

providers, who in turn used a portion of the payment to engage Defendant's services, including Defendant's guardianship of the Personal and Medical Information.

208. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant when it accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of Personal and Medical Information to Defendant from Plaintiff's and Class Members' healthcare or insurance providers is an integral part of Defendant's business. Without collecting and maintaining Plaintiff and Class Members' Personal and Medical Information, Defendant would have dramatically diminished business and profits.

209. Defendant was supposed to use some of the monetary benefit provided to it from Plaintiff and Class Members to secure the Personal and Medical Information belonging to Plaintiff and Class Members by paying for costs of adequate data management and security.

210. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement necessary security measures to protect the Personal and Medical Information of Plaintiff and Class Members.

211. Defendant gained access to the Plaintiff's and Class Members' Personal and Medical Information through inequitable means because Defendant failed to disclose that it used inadequate security measures.

212. Plaintiff and Class Members were unaware of the inadequate security measures and would not have entrusted their Personal and Medical Information to Defendant had they known of the inadequate security measures.

213. To the extent that this cause of action is pled in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

214. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Personal and Medical Information is used; (iii) the compromise and/or theft of their Personal and Medical Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal and Medical Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Personal and Medical Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Personal and Medical Information of Plaintiff and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal and Medical Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

215. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

216. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds from the monetary benefit that it unjustly received from them.

COUNT VI

DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

217. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

218. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

219. As previously alleged, Plaintiff and members of the Class entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the Personal and Medical Information it collected from Plaintiff and the Class.

220. Defendant owes a duty of care to Plaintiff and Class members that require it to adequately secure Plaintiff's and Class members' Personal and Medical Information.

221. Defendant still possesses the Personal and Medical Information of Plaintiff and the Class members.

222. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

223. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their Personal and Medical Information and Defendant's failure to address the security failings that led to such exposure.

224. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

225. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant provide employee training regarding the dangers and risks inherent in using file-sharing websites like the Website at issue here to store and/or transmit Personal and Medical Information;

e. Ordering that Defendant cease transmitting Personal and Medical Information via file-sharing websites like the Website at issue here;

f. Ordering that Defendant cease storing Personal and Medical Information on file-sharing websites like the Website at issue here;

g. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Personal and Medical Information not necessary for its provision of services;

h. Ordering that Defendant conduct regular database scanning and security checks; and

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, patient personally identifiable information and patient protected health information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personal and Medical Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal and Medical Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five (5) years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, nominal damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Dated: September 13, 2022

Respectfully submitted,

/s/ William B. Federman
William B. Federman
John C. Sherwood
FEDERMAN & SHERWOOD
212 W. Spring Valley Rd.
Richardson, TX 75081
Telephone: (214) 239-4568
Facsimile: (281) 254-7789
-and-
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com
jsherwood@sherwoodlawoffice.com

A. Brooke Murphy
(*Pro hac vice* application forthcoming)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Counsel for Plaintiff and the Putative Class